

REVERSIBLE IMAGE STEGANOGRAPHY
USING ROI & RONI

LIM JEE CHAO

BACHELOR OF COMPUTER SCIENCE

UNIVERSITI MALAYSIA PAHANG



SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor Computer Science (Software Engineering)

A handwritten signature in black ink, appearing to read 'LSC' or similar, positioned above a horizontal line.

(Supervisor's Signature)

Full Name : Dr. Liew Siau Chuin
Position : Senior Lecturer
Date : 03/01/2019



STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

A handwritten signature in black ink, appearing to be "JC" or similar, written above a horizontal line.

(Student's Signature)

Full Name : Lim Jee Chao
ID Number : CB15010
Date : 03/01/2019

REVERSIBLE IMAGE STEGANOGRAPHY
USING ROI & RONI

LIM JEE CHAO

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor of Computer Science (Software Engineering)

Faculty of Systems Computer & Software Engineering
UNIVERSITI MALAYSIA PAHANG

JANUARY 2019

ACKNOWLEDGEMENTS

First of all, I am grateful and would like to thank my supervisor, Dr. Liew Siau Chuin for his continuous encouragement, outstanding advice and guidance in conducting this research. I am appreciated for his patience in spending a lot of time to guide me and give a lot of useful suggestions during this period.

Next, I would like to appreciate to my friends who supported and gave their knowledge to me. I would like to express my high appreciation to all lecturers and friends that have guided me. Lastly, I am very grateful to my family for their endless support.

ABSTRAK

Reversible steganography dapat memulihkan imej asal tanpa ada penyelewengan apabila mesej rahsia tertanam telah diekstrak. Kajian ini telah diuji dengan empat imej yang berbeza dan satu storan imej. Imej sampel dibahagikan kepada tiga jenis rantau iaitu *Region of Interest (ROI)*, *Region of Non-Interest (RONI)* dan rantau yang tak tersentuh. Penyelidikan ini menggunakan teknik mencari *ROI* dan *RONI* untuk mencari kedudukan untuk membenamkan mesej dan memulihkan imej asal. Semasa proses pembenaman, *bit RONI* disimpan ke dalam imej storan yang dikenali sebagai *sample_image*. Seterusnya, *bit ROI* disimpan ke *RONI* supaya ia dapat pulih semasa proses pengekstrakan. Pengirim memilih koordinat x dan koordinat y untuk membenamkan maklumat rahsia ke dalam *ROI2*. Pengirim juga perlu membenamkan kunci rahsia dalam imej *RONI2* yang boleh membantu untuk mendapatkan maklumat rahsia. Selepas itu, *stego-imej* dihasilkan selepas *ROI* dan *RONI* tertanam. Dalam proses pengekstrakan, penerima perlu mengekstrak kunci rahsia untuk menyahsulit mesej rahsia. Untuk proses balik, *ROI* dan *RONI* dibalikkan kepada *bit* asal. *Peak Signal-to-Noise Ratio (PSNR)* digunakan untuk mengukur kualiti *stego-imej* dan kesamaan imej asal dan memulihkan imej. Nilai *PSNR* daripada empat imej sampel terpilih adalah antara 52.60dB hingga 52.62dB. Histogram imej asal, *stego-imej* dan imej pulih dijana untuk perbezaan visual antara imej asal, *stego-image* dan memulihkan imej. Kesimpulannya, kaedah yang dicadangkan ini telah membuktikan pendekatan yang lebih baik berbanding dengan kerja sebelumnya dari segi memilih kedudukan untuk membenamkan dengan menggunakan *ROI* dan *RONI*.

ABSTRACT

Reversible steganography allows to recover of original image without any distortion when the embedded secret message has extracted. This research was tested with four different image and one storage image. The sample image is divided into three type of region which are Region of Interest (ROI), Region of Non-Interest (RONI) and untouchable region. This research using the technique of finding the ROI and RONI of the cover image to find position to embed the message and recover the original image. During embedding process, the RONIs' bits are stored into the storage image known as sample_image. Next, the ROIs' bits are stored into RONI so that it can be recovered during extraction process. Sender select the x-coordinate and y-coordinate to embed the secret information into the ROI2. Sender also need embed the secret key in the RONI2 image which can help to secure the secret information. After that, stego-image was generated after ROI and RONI embedded. In extraction process, receiver need to extract the secret key to decrypt the secret message. For reversible process, ROIs and RONIs were reversed to original bits. Peak Signal-to-Noise Ratio (PSNR) value was used to measure the quality of stego-image and similarity of original image and recover image. The value of PSNR of the four selected sample image is between 52.60dB to 52.62dB. Histogram of original image, stego-image and recover image are generated for visual difference between original image, stego-image and recover image. In conclusion, this proposed method has proved a better approach compared to previous work in terms of selecting a position to embed by using ROI and RONI.

TABLE OF CONTENT

DECLARATION

TITLE PAGE

ACKNOWLEDGEMENTS **ii**

ABSTRAK **iii**

ABSTRACT **iv**

TABLE OF CONTENT **v**

LIST OF TABLES **viii**

LIST OF FIGURES **ix**

LIST OF ABBREVIATIONS **xii**

CHAPTER 1 INTRODUCTION **1**

1.1 Introduction 1

1.2 Problem Statement 2

1.3 Objectives 2

1.4 Scope 2

1.5 Significant 3

1.6 Thesis Organization 3

CHAPTER 2 LITERATURE REVIEW **4**

2.1 Introduction 4

2.2 Overview of Steganography 4

2.3 Reversible Steganography Techniques 6

2.4 Peak Signal to Noise Ratio 7

2.5	Existing Method in Reversible Steganography	8
2.5.1	Reversible Data Hiding (RDH)	8
2.5.2	High Capacity Reversible Steganography using Multilayer Embedding (CRS)	10
2.5.3	High Capacity and Adaptive Steganographic Algorithm based on Novel Image Interpolation (RAS)	12
2.6	Conclusion	14
CHAPTER 3 METHODOLOGY		15
3.1	Introduction	15
3.2	Methodology	15
3.2.1	Least Significant Bit (LSB)	15
3.2.2	Image used and Secret Information File	16
3.2.3	Secret Key Preparation	20
3.2.4	Embedding Process	21
3.2.5	Extracting Process	23
3.3	Hardware and Software	25
3.4	Gantt Chart	25
3.5	Implementation	26
3.5.1	Example of Secret Text File in Roni	26
3.5.2	Algorithm	28
CHAPTER 4 RESULT & DISCUSSION		30
4.1	Introduction	30
4.2	Process of Reversible Steganography	30
4.2.1	Image and Text Preparation	31
4.2.2	Storage Image Embedding	37

4.2.3	Text Embedding	38
4.2.4	Text Extraction	39
4.2.5	Reversible Steganography	40
4.2.6	Embedding Capacity	40
4.3	Experimental Result	41
4.3.1	Message Embedding and Extraction	45
4.3.2	Reversible Steganography	51
4.4	Discussion	60
CHAPTER 5 CONCLUSION		62
5.1	Introduction	62
5.2	Conclusion	62
5.3	Research Constraint	63
5.4	Future Work	64
5.5	Summary	64
REFERENCES		65
APPENDIX A GANTT CHART		67

LIST OF TABLES

Table 2.1 PSNR value of Wu H., J. Dugelay, and Y. Shi, 2015 method	9
Table 2.2 PSNR value of M. Tang, J. Hu. & W. Song,2014 method	11
Table 2.3: PSNR value of M. Tang, J. Hu, W. Song and S. Zeng,2015 method	13
Table 2.4 Comparison of PSNR between Lena Images in Reversible Steganography Methods	14
Table 3.1 Hardware Requirements	25
Table 3.2 Software Requirements	25
Table 4.1 Secret Text File	31
Table 4.2 Details of Secret Key	31
Table 4.3 Details of lena.bmp and divided regions	32
Table 4.4 Details of peppers.bmp and divided regions	33
Table 4.5 Details of baboon.bmp and divided regions	34
Table 4.6 Details of zelda.bmp and divided regions	35
Table 4.7 PSNR of each steganography image and average PSNR	45
Table 4.8 Experiment 1: Total bits to be embedded is less than ROI2 image	46
Table 4.9 Experiment 2: Total bits to be embedded is larger than ROI2 image	47
Table 4.10 Experiment 3: Total bits to be embedded is less than RONI2 image	48
Table 4.11 Experiment 4: Total bits to be embedded is larger than ROI2 image	49
Table 4.12 Comparison of selected pixels from ROI2	53
Table 4.13 Comparison of selected pixels from RONI1	55
Table 4.14 Comparison of selected pixels from RONI2	57

LIST OF FIGURES

Figure 2.1	Steganography scheme	5
Figure 2.2	Reversible Steganography scheme	6
Figure 2.3	Process of the RDH algorithm	8
Figure 2.4	3 x 3 blocks of interpolating image	10
Figure 2.5	3 x 3 overlapping blocks of interpolating image	12
Figure 3.1	1 st position of Least Significant Bits in pixel	15
Figure 3.2	lena.bmp	16
Figure 3.3	peppers.bmp	16
Figure 3.4	baboon.bmp	17
Figure 3.5	zelda.bmp	17
Figure 3.6	sample of ROI1 (120 x 120 pixels)	17
Figure 3. 7	The layout of cover image	18
Figure 3.8	sample of cover image divide into ROI, RONI and untouchable region	18
Figure 3.9	Secret Text File (myfile.txt)	19
Figure 3.10	ASCII Code	20
Figure 3.11	Convert user input to hexadecimal and binary values	20
Figure 3.12	Flowchart of embedding process	22
Figure 3.13	Flowchart of extracting process	24
Figure 3.14	Sample of pixel value in hexadecimal number	26
Figure 3.15	Sample of pixel value in binary number	26
Figure 3.16	Sample of secret message	27
Figure 3.17	Sample of embedded message into a stego-image	27
Figure 4.1	lena.bmp	32
Figure 4.2	Lena ROI1	32
Figure 4.3	Lena ROI2	32
Figure 4.4	Lena RONI1 and RONI2	32
Figure 4.5	pepper.bmp	33
Figure 4.6	Peppers ROI1	33
Figure 4.7	Peppers ROI2	33
Figure 4.8	Peppers RONI1 and RONI2	33
Figure 4.9	Baboon.bmp	34
Figure 4.10	Baboon ROI1	34

Figure 4.11	Baboon ROI2	34
Figure 4.12	Baboon RONI1 and RONI2	34
Figure 4.13	zelda.bmp	35
Figure 4.14	Zelda ROI1	35
Figure 4.15	Zelda ROI2	35
Figure 4.16	Zelda RONI1 and RONI 2	35
Figure 4.17	Storage image to keep original bits of RONI1 and RONI 2 (1300x1300 pixels)	36
Figure 4.18	Illustration of image embedded	37
Figure 4.19	Illustration of message and secret key embedded	38
Figure 4.20	Illustration of message and secret key extraction	39
Figure 4.21	Illustration of reversible steganography	40
Figure 4.22	Stego-image of lena.bmp, PSNR = 52.6054dB	41
Figure 4.23	Stego-image of peppers.bmp, PSNR = 52.6207dB	42
Figure 4.24	Stego-image of baboon.bmp, PSNR = 52.6174dB	42
Figure 4.25	Stego-image of zelda.bmp, PSNR = 52.6143dB	42
Figure 4.26	Histogram of Original Lena and Encrypted Stego-image Lena	43
Figure 4.27	Histogram of Original Peppers and Encrypted Stego-image Peppers	43
Figure 4.28	Histogram of Original Baboon and Encrypted Stego-image Baboon	44
Figure 4.29	Histogram of Original Zelda and Encrypted Stego-image Zelda	44
Figure 4.30	The message file to embed in ROI2 image (348 characters)	49
Figure 4.31	The message that extract in encrypt file.	49
Figure 4.32	The message file to embed in ROI2 image (630 characters)	50
Figure 4.33	The message that extract first 2601pixels in decrypt file.	50
Figure 4.34	User key in the secret key that extract from RONI2.	50
Figure 4.35	User key in the correct key will get the secret message	50
Figure 4.36	User input wrong password will get the error message	50
Figure 4.37	Selected ROI2 region of Lena image	52
Figure 4.38	Selected ROI2 region of Lena image after embedded the secret message	52
Figure 4.39	Selected ROI2 region of Lena image after reversible	53
Figure 4.40	Selected RONI1 region of Lena image	54
Figure 4.41	Selected RONI1 region of Lena image after embedded the original bit of ROI1	54
Figure 4.42	Selected RONI1 region of Lena image after reversible	55
Figure 4.43	Selected RONI2 region of Lena image	56

Figure 4.44	Selected RONI2 region of Lena image after embedded the secret key	56
Figure 4.45	Selected RONI2 region of Lena image after reversible	57
Figure 4.46	Histogram of Original Lena and Recover Lena	58
Figure 4.47	Histogram of Original Peppers and Recover Peppers	58
Figure 4.48	Histogram of Original Baboon and Recover Baboon	59
Figure 4.49	Histogram of Original Zelda and Recover Zelda	59
Figure 4.50	PSNR and MSE of reversed image of Lena	61

LIST OF ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
bmp	Bitmap format file
dB	Decibels
DWT	Discrete Wavelet Transform
LSB	Least Significant Bit
MSE	Mean Squared Error
PSNR	Peak Signal-to-Noise Ratio
ROI	Region of Interest
RONI	Region of Non-Interest

CHAPTER 1

INTRODUCTION

1.1 Introduction

Steganography is a type of technique of hiding some information into a media such as video, text, audio and image. Steganography technique can let us use secret information communication to others. This technique allows us send hidden an encrypted message inside another file to receiver so that can avoid detected, stolen, or destroyed by third party. Reversible steganography allows to recover of original image without any distortion when the embedded secret message has extracted. There are two types of reversible steganographic techniques which spatial domain and transform domain. In spatial domain, the Least Significant Bits (LSB) is the most common and simple approach for embedding message in a cover image. It is used the least significant bit of every pixel value in the image. Least Significant Bit is the simplest and easiest way of hiding information. In transform domain, it is a complex way to hide the information into the cover image compare with spatial domain. It transferred the cover image into another transformation and apply data hiding technique on it. There have two type methods in transform domain which Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT). DCT embeds the information by altering the transformed DCT co-efficient. DWT work by talking many wavelets to encode the image.

Steganography technique allow hiding information in the image. After embedded secret message into the image, we cannot recover the original image. Hence, we use reversible steganography technique which allows to extract hidden data and recover the original image.

1.2 Problem Statement

When using steganography technique, it will replace the stego-image to the original image. If delete the secret message from stego-image, it still cannot get back the original image. Therefore, steganography method needs to make sure are reversible and the original image can be used repeatedly.

Hence, technique on finding, hide secret information and recover original image on Region of Interest and Region of Non-Interest is proposed. This method prevents data hiding method are irreversible and user can recover the original image.

1.3 Objectives

- i. To study current reversible image steganography technique.
- ii. To propose reversible image steganography using LSB technique.
- iii. To test the reversibility steganography technique to recover the original image.

1.4 Scope

- i. Reversible Image Steganography technique only focuses on grayscale image.
- ii. Demonstrate to ROI and RONI technique to recover original image.
- iii. Test the reversibility steganography technique.

1.5 Significant

- i. Sender and receiver can recover the original image on reversible image steganography technique.
- ii. This research project help to improve the quality of original image.
- iii. To help hiding some information into an image.

1.6 Thesis Organization

This project consists of five chapters. Chapter 1 is research introduction. Chapter 2 is a literature review. Chapter 3 is the methodology of this research. Chapter 4 is implementation, testing and result in discussion. Chapter 5 is the conclusion of this research.

REFERENCES

- Akinola, S. O., & Olatidoye, A. A. ON THE IMAGE QUALITY AND ENCODING TIMES OF LSB, MSB AND COMBINED LSB-MSB STEGANOGRAPHY ALGORITHMS USING DIGITAL IMAGES.
- Atawneh, S. (2006). *A new algorithm for hiding gray images using blocks*. Paper presented at the Information and Communication Technologies, 2006. ICTTA'06. 2nd.
- Bhallamudi, S. (2015). Image Steganography Final project–Report.
- Hu, J., & Li, T. (2015). Reversible steganography using extended image interpolation technique. *Computers & Electrical Engineering*, 46, 447-455.
- Kaur, S., & Shukla, M. (2014). Reversible data hiding and its methods: a survey. *International Journal of Computer Science and Mobile Computing*, 3(5), 821-826.
- Lee, C.-F., & Huang, Y.-L. (2012). An efficient image interpolation increasing payload in reversible data hiding. *Expert Systems with Applications*, 39(8), 6712-6719.
- Sajna, U. (2014). LSB STEGANOGRAPHY BASED REVERSIBLE DATA HIDING'. *International Journal of Advances in Engineering & Technology*, 7(1), 105-112.
- Sarkar, T., & Sanyal, S. (2014). Reversible and irreversible data hiding technique. *arXiv preprint arXiv:1405.2684*.
- Tamimi, A. A., Abdalla, A. M., & Al-Allaf, O. (2013). Hiding an image inside another image using variable-rate steganography. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 4(10).
- Tang, M., Hu, J., & Song, W. (2014). A high capacity image steganography using multi-layer embedding. *Optik-International Journal for Light and Electron Optics*, 125(15), 3972-3976.

- Tang, M., Hu, J., Song, W., & Zeng, S. (2015). Reversible and adaptive image steganographic method. *AEU-International Journal of Electronics and Communications*, 69(12), 1745-1754.
- Walia, E., Jain, P., & Navdeep, N. (2010). An analysis of LSB & DCT based steganography. *Global Journal of Computer Science and Technology*.
- Wu, H.-T., Dugelay, J.-L., & Shi, Y.-Q. (2015). Reversible Image Data Hiding with Contrast Enhancement. *IEEE Signal Process. Lett.*, 22(1), 81-85.
- Zeng, X.-t., & Li, Z. (2012). Reversible data hiding scheme using reference pixel and multi-layer embedding. *AEU-International Journal of Electronics and Communications*, 66(7), 532-539.
- Zhang, Z., & Zhang, W. (2015). *Reversible steganography: Data hiding for covert storage*. Paper presented at the Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2015 Asia-Pacific.